Questions for the Record
Nuala O'Connor, President and CEO
Center for Democracy and Technology

Protecting Consumer Privacy in the Era of Big Data
Subcommittee on Consumer Protection and Commerce
House Energy and Commerce
February 26, 2019

1. In the wake of the repeal of broadband privacy rules last year, what are your thoughts on privacy proposals including ISPs. For example, should ISPs be able to mine DNS data? Are there any other solutions to this that could protect consumers from these privacy violations if we don't come up with a regulatory one?

The United States should have a universal privacy law that applies to all actors, including internet service providers (ISPs) and other types of businesses, online and offline. People should be able to rely on basic protections that follow their data no matter who holds or processes it. The repeal of the broadband privacy rules in 2017 adds to the urgency of passing comprehensive privacy legislation. ISPs have access to and process highly sensitive personal information by virtue of providing a vital location-based service. Privacy legislation should protect much of this information from secondary uses, which in the context of ISPs means uses that are not required to provide the internet access or other services which a consumer has chosen. CDT's draft legislation contains several key data use and sharing prohibitions that would protect broadband customers, but that, more importantly, would also apply to the entire data ecosystem.

First, our proposal prohibits the processing of precise geolocation information if it is not required to provide the service a person has requested (such as broadband internet service). Data that customers send to ISPs by virtue of using the internet can reveal their location. To the extent that this location information is precise (within 1,750 feet), our bill would prohibit any entity from collecting, sharing, selling, or otherwise processing it except as necessary to provide the service.

Second, our proposed bill allows the processing of health information only when it is necessary to provide the service a person has requested, such as a health or fitness tracking app or a symptom-checking tool. This means companies may process information as necessary to provide and optimize broadband service, but may not harvest health data and share it with advertisers. A person's browsing and app usage history—the websites and pages they visit, search history, and names or categories of apps they use and information they send to those apps—can reveal personal health information (for example, if a person is reading about a particular health condition, purchasing healthcare products, using a wearable fitness device or sleep tracking app). Consumers should be able to access health-related information and services without worrying that this information could end up in the hands of third parties, be

used to serve them third-party ads, or determine the types and rates of insurance or credit for which they qualify.

Third, our proposed legislation prohibits the sale or licensing of the contents of or parties to communications. This would include browsing information, such as the websites a person visits, the messages (such as emails, texts, and instant messages) they send, and the individuals they communicate with. The sale of browsing history was a central concern that led the Federal Communications Commission (FCC) to write broadband privacy rules. Many different types of companies and services process browsing history, and it should be protected regardless of the type of entity processing it.

Domain Name System (DNS) data can reveal the contents of people's online activities, including the websites they visit. This type of data would be covered by the secondary use prohibitions in CDT's draft legislation.

While individuals may be able to take certain steps to obscure some of their browsing history, such as using a virtual private network (VPN), no self-help solution can give people complete control over the sensitive personal information that they must reveal in order to participate in digital life. VPNs themselves are provided by companies that customers must trust to protect their information. Even when websites encrypt their traffic, DNS data can still reveal nuanced information about people's activities. Ultimately, Congress must pass legislation to limit the behavior of ISPs and all other entities that process personal information.

2. Many proposals direct the FTC to establish rules to address advertising practices that result in discrimination. Do you have ideas in mind for what kind of rules the FTC could put in place?

The Federal Trade Commission (FTC) should request and analyze corporate information about advertising targeting practices and develop rules that address discriminatory or otherwise unfair advertising practices. Because there is a lack of transparency into the online advertising ecosystem, more information is needed to fully understand the types of data collection, aggregation, sharing, profiling, and targeting practices that result in discrimination or exploitation. The FTC has indicated that it intends to launch a study of platforms' data practices. The activities of advertising networks, data brokers, and advertisers themselves must also be considered.

Some findings about discriminatory advertising and potential responses are beginning to emerge through litigation. Last week, Facebook reached a settlement in lawsuits alleging that its practices relating to the advertising of jobs and housing violated civil rights laws. As part of the settlement, Facebook agreed to several changes, including creating a separate portal for users placing job, credit, and housing ads, which will restrict targeting options. Advertisers in these categories will no longer have the option of excluding people based on age, gender, zip code, and several other categories. Facebook will also create a portal where users can search and view all current housing ads that have been placed, regardless of the advertisers' targeting

choices. Facebook will also allow the National Fair Housing Alliance to engage in testing of the platform to ensure that these reforms are effective. While these are first steps that only address one part of the market for potentially discriminatory advertising, they are measures whose effectiveness the FTC can observe over the next several months or years as the agency crafts rules. In particular, the ability to test or audit companies' practices has long been a critical aspect of enforcing civil rights laws in the brick and mortar world, and we would encourage the FTC to consider how testing can and should be done online.